HADMÉRNÖK

VIII. Évfolyam 3. szám - 2013. szeptember

Kassai Károly
karoly.kassai@hm.gov.hu

AZ ELEKTRONIKUS INFORMÁCIÓBIZTONSÁGI KÉRDÉSEK MEGJELENÉSE A MAGYAR HONVÉDSÉG HÍRADÓ-INFORMATIKAI SZABÁLYZATBAN

Absztrakt

A híradó és informatikai szabályzásnak le kell fednie minden területet a stratégiai szintű műveletektől a harcászati szintű műveletekig itthon és külföldön támogatva a vezetési és irányítási képességeket a minősített vagy nem minősített adatkezelés érdekében a parancsnokok követelményei szerint. A másik kritikus tényező a híradó és informatikai rendszerek támogatása és az információbiztonsági szempontok közötti összehangolás. A szerző szándéka a biztonsági követelmények beillesztésének támogatása a tervezett új híradó és informatikai szabályzatba, valamint a stratégiai szinten az alapvető biztonsági filozófia megértésének segítése.

The CIS regulation has to cover all issues from strategic level to tactical level operations at home and abroad, supporting C2 capabilities to handle classified and unclassified information according to the requirements of commanders. The other critical factor is the coordination between CIS support and the CIS security point of view. The intention of the author is to support the implementation of security requirements into the planned future CIS regulation and to help to understand the basic security philosophy at strategic level.

Kulcsszavak: *információbiztonság, elektronikus információbiztonság, kiberbiztonság, szabályozás ~ information security, electronic information security, cyber security, regulation.*

ELŐZMÉNYEK

A Magyar Honvédségnél (MH) a híradó és informatikai kérdések szabályozása több, korábban kiadott szabályzat és alacsonyabb szintű belső rendelkezés feladata.[1]

A jelenlegi rend szerint az informatikai szakterület első számú szabályozója az 1993-ban kiadott MH Informatikai Szabályzat [1], mely az akkori szervezeti kultúrának megfelelően keretet adott az informatikai szakkérdések kezelésének, benne az elektronikus információbiztonságra vonatkozó alapvető követelményeket is megfogalmazva.

Vezérkar főnöki intézkedésben megtörtént a szakterületi kérdések korszerű szabályzatban történő kidolgozásának elrendelése a közelmúltban, így a jól felépített, logikus – de már korszerűtlen – „kis zöld" helyett jövőre kiadásra kerül a Magyar Honvédség Híradó-informatikai Szabályzata (továbbiakban: Szabályzat), melynek kidolgozása a 2013. július 29-én egyeztetett, jóváhagyásra felterjesztett szinopszissal megkezdődött. [2]

A kidolgozás tartalmi elemeiről hírt adni ilyen rövid idő elmúltával nem lehetséges, de a téma fontossága és az elektronikus információbiztonsági szakterülettel való szoros kapcsolat szükségessé teszi e szabályozási feladat kapcsán néhány elektronikus információbiztonsági szempont vizsgálatát.

A legelső szembeötlő változás maga a cím, ami jelzi, hogy a korábbi szakterületi elkülönülést a szakmai feladatok vezetéséért felelős HM szerv és a szakfeladatokat végrehajtó szervezetek a továbbiakban nem kívánják fenntartani. Ez a törekvés szinkronban van a világban történő eseményekkel, hadtudományi és egyéb szakterületi megállapításokkal. Napjaink egyre jobban digitálissá váló életünkben már egyre nehezebb az analóg vagy digitális átviteli út, vagy adat és hangkommunikáció – esetleg más szempontok – szerint „híradó" és „informatika" területekre osztani a világot.

A Szabályzat másik érdekessége – ami egyben a megoldandó feladat nehézségét is jelzi–, hogy a híradó és informatikai szakterületeken definiáltan még nem alakult ki az szabályozási hierarchia, ami az „általánostól az egyedi felé" elv alapján tartalmazza, hogy a szakmapolitika – általános, központi követelmények – rendszer vagy funkcionális alapon kiadott alacsonyabb szintű és szűkebb hatókörű szakutasítások rendjében milyen szabályozót, belső rendelkezést kell kialakítani. A kidolgozás így magában hordozza azt a kihívást, hogy már meglévő szabályozót kell módosítani, vagy meglévő (esetleg kialakulás alatt álló) értékes szabályozó elemeket kell megbontani annak érdekében, hogy később kialakítandó alacsonyabb szintű szabályozóba tartozó, részletesebben megfogalmazott követelmények ne kerüljenek be a központi Szabályzatba.

A Szabályzat szinopszisa szakmai egyetértés alapján jóváhagyott kiindulási pont, de a kidolgozás menete során értelemszerűen változhat, formálódhat, ami miatt nem célszerű elemzése, értelmezése. Érdekes kérdésnek csak az mutatkozhat, hogy a híradó és informatikai szakterületek mennyire tartják fontosnak a nemzetközi, nemzeti szabványok és „bevált gyakorlat" körébe tartozó ajánlások alkalmazását. A szabványkövetés kérdése figyelmet érdemel, mert a nemzetközi szakirodalomban az elektronikus információbiztonságra vonatkozó irányadó szabványok illeszkednek a katonai terminológia szerint „híradó és informatikai" szabályozáshoz, így könnyen elkerülhető a „keresztbe szabályozás" vagy egyéb szakterületi összehangolatlanságot okozó probléma. E miatt elektronikus információ biztonság szempontjából (is) fontos kérdés a híradó és informatikai szakterület szabványkövetésre vonatkozó döntése, ami a kidolgozásról szóló döntés során sikeresen meg is született. A kérdés érdekessége és a kidolgozók felelősségét, a szabályozási munka nehézségét jelzi, hogy az MH-ra is érvényesíthetően az informatika, vagy távközlés területén teljes körű, jogszabályban

[1] A szerző korábbi cikke – az elektronikus információbiztonságra koncentrálva – átfogó jelleggel azonosította a szabályozókat: Az elektronikus információvédelem szabályozási kérdései a közelmúltban, Hadmérnök, VIII. évfolyam 1. szám, 2013. március, p. 203-214.

megfogalmazott követelmények, kötelezően alkalmazandó szabványok vagy ajánlások nem azonosíthatók (még a kormányzati célú hálózatokról szóló jogszabály sem azonosít ilyen követelményeket). [3] E mellett az elektronikus információbiztonság területén a NATO és EU követelmények mellett törvény és kormányrendelet szabályozza a minősített adatkezelésre vonatkozó követelményeket, illetve 2013. július elsejétől az állami és önkormányzati szervezetek elektronikus információbiztonságáról is jogszabály rendelkezik (Ibtv.) **Hiba! A hivatkozási forrás nem található.**, ami jelzi a szakterületek közötti összehangolás fontosságát.

Az előzményekhez tartozóan utolsó kérdésként meg kell említeni a tervezett Szabályzat és az elektronikus információbiztonság szakterületi kapcsolatát, illetve azt a kérdést, hogy tervezett Szabályzat tartalmazzon-e az elektronikus információbiztonságra – illetve tágabban: információbiztonságra – vonatkozó részeket (és milyen mértékben), vagy nem.

A kidolgozásért felelős híradó és informatikai szakterületi képviselők állásfoglalása szerint az elektronikus információbiztonsági kérdések szabályozással e Szabályzat kidolgozása nem ütközhet a már meglévő biztonsági területű szabályozókkal. Ezzel együtt híradó és informatikai szakterületi igényként fogalmazódott meg, hogy elektronikus információbiztonságra – illetve tágabban: információbiztonságra – vonatkozó fejezetet kell a Szabályzatnak tartalmaznia. Az információbiztonsági fejezetben meg kell fogalmazni a fizikai, személyi, adminisztratív és elektronikus információbiztonsággal[2] kapcsolatosan azokat az alapkérdéseket, melyek *általános követelmények szintjén iránymutatást adnak a híradó és informatikai szakállománynak és megfogalmazásával segítik, hogy milyen információbiztonsági területű szabályozót „kell kézbe venni" az adott kérdés megoldása érdekében*, vagy *milyen irányon kell segítséget kérni*, ha technológiai váltás vagy nem szabályozott kérdés miatt eddig ismeretlen helyzetet kell megoldani.

A cikk a továbbiakban a Szabályzatban megjelenítendő elektronikus információ biztonsági részek előkészítését szolgálja. Cél, hogy az elektronikus adatfeldolgozás támogatása érdekében a rendszerek, szolgáltatások teljes életciklusán keresztül látható legyen az a biztonsági szemléletmód, amely biztosítja az adatok és rendszerek szükséges mértékű biztonságát. Az elektronikus adatfeldolgozás területén ez az elektronikus információbiztonsági keretrendszer egyaránt tartalmazza a minősített és nem minősített adatok körét, valamint a NATO, EU és más két vagy többoldalú szerződés védelme alatt álló, vagy nemzeti adatot.

A HADMŰVELETI KÖVETELMÉNYEK, FELHASZNÁLÓI IGÉNYEK BIZTONSÁGI SZEMPONTJAI

Az elektronikus adatkezelő rendszerek, képességek biztonsága szempontjából az egyik legfontosabb kérdés az első lépések, döntések és szerepük fontosságának tisztázása. *Új szolgáltatásokat biztosító elektronikus adatkezelő rendszerek kialakítása, vagy meglévő rendszerek változtatása csak jóváhagyott követelmények alapján történhet.* Ez a követelmény gyakran azért kerül ki a nézőpontból, mert túlnyomórészt meglévő rendszerek módosításai, fejlesztései képezik a változások zömét, melynek során gyakori a rendszer meglévő tartalékaira való támaszkodás, vagy racionalizálásból adódó erőforrás felhasználásra történő hivatkozás, mely lehetőségek elvonják a figyelmet az erőforrások biztosításának szükségességéről.

A „hadműveleti követelmények" és a „felhasználói igények" kapcsolata izgalmas vizsgálandó kérdés, mert az egyéni felhasználói igények nem írhatják felül a vezetési és irányítási képességekre vonatkozó magasabb szintű központi követelményeket.

[2] A kérdés szakmai kihívásnak tekinthető, mert jogszabály jelenleg csak a minősített adatok kezelése területén azonosít fizikai, személyi és adminisztratív jellegű követelményeket, [5][6] így az MH esetében e szabályokat a szervezetre vonatkozóan, önállóan kell megalkotni. E területen változtatást fog jelenteni az Ibtv. végrehajtását célzó NFM rendelet megjelenése, bár jelenleg még pontosan nem azonosítható a rendelet tervezet hatóköre.

Nemzeti viszonylatban a hadműveleti szakterület feladata az MH összes szervezetére meghatározni és jóváhagyatni a békeidőszakra vonatkozó vezetési és irányítási rendet, lefektetni az alapokat a különleges jogrendben szükséges vezetési és irányítási képességek meghatározása érdekében. *Ez a nemzeti keretrendszer csak a NATO és EU követelményekkel összhangban alakítható ki*, mivel a missziós kötelékek, vagy a NATO felajánlott erők kategóriájába tartozó képességeknek rendelkeznie kell a szövetséges előírások szerinti elöljárói, együttműködő és adminisztratív támogató kapcsolatokkal.

A vezetési képességekre vonatkozóan a feladat jellege, a környezet és egyéb változók miatt a kötelező jellegű szolgáltatásokon belül – vagy azok kiegészítéseként – megjelenhetnek szervezeti vagy egyéni igények, melyek a kiegészítéshez vagy módosításhoz szükséges erőforrások megléte és a biztonsági feltételrendszer kialakíthatósága esetén módosíthatják a szolgáltatások körét, a szolgálati vagy magáncélú adatkezelési lehetőségeket. E területen kritikus fontosságú annak tudatosítása, hogy *az erőforrások ideális esetben a központi hadműveleti követelményeknek megfelelően kialakítottak. Az esetleges változások, kiegészítések erőforrás szempontjából nem csak eseti kiadásokat vagy feladatokat jelentenek, hanem a további életciklus szakaszok alatt is erőforrásokat igényelnek*, melyek hiánya esetén az adott szolgáltatás csak ideig-óráig lesz elérhető.

A hadműveleti követelményeknek, felhasználói igényeknek tartalmaznia kell a biztonsági követelmények meghatározásához szükséges alapadatokat. A minimálisan meghatározandó adatok:

- a felhasználói kör és a szükséges személyi biztonsági követelmények;
- a kezelt adatok típusa (hang, adat, kép stb.), formátuma és a szükséges adatkezelő szolgáltatások, beleértve a más rendszerek felé történő egyoldalú vagy kölcsönös adatcsere igényeket;
- a kezelt adatok biztonsági osztálya, minősítési szintek és kezelési utasítások, hozzáférési korlátozások;
- adatkezelési helyszínek;
- a rendelkezésre állásra vonatkozó követelmények és prioritások (szolgáltatás, adat).

Az elektronikus adatkezelő rendszerre vonatkozó hadműveleti követelmények változtatása, pontosítása során vizsgálni kell a kockázatokat, és azok vezetésre és irányításra kifejtett biztonsági hatásait. Az elfogadható kockázatokat, illetve a változás okán keletkező, de erőforrások igénybevételével ellensúlyozható kockázatokat jóvá kell hagyatni. Ez a rendszabály azt célozza, hogy a követelményeket meghatározó vezető kapja meg a változást okozó döntések következményeivel járó információkat, rendelje el a változások okozta védelmi rendszabályok módosítását és tudatosan vállalja az információs kockázatokat.

A BIZTONSÁGI SZEMPONTOK ÉRVÉNYESÍTÉSE A TERVEZÉS, KIALAKÍTÁS, ÜZEMELTETÉS ÉS FEJLESZTÉS SORÁN

Nagy gyakorlatot igényel annak helyes mérlegelése, hogy mely tervezési, tesztelési vagy üzemeltetési feladat igényel elektronikus információbiztonsági támogatást, és melyek azok az esetek, amikor egy gyors konzultáció vagy dokumentálás kielégíti a biztonsági szempontú megfelelőséget.

Az elektronikus adatkezelő rendszerek tervezésekor a legkorábbi szakaszban meg kell jeleníteni és érvényesíteni kell a biztonsági szempontokat.

Az elektronikus adatkezelő rendszerek tervezési, fejlesztési, kialakítási és üzemeltetési fázisaiban azonosítani kell a szakfeladatokért való felelősségeket, és azokat úgy kell összehangolni, hogy a felelősség pontosan azonosítható legyen. A biztonsági követelmények, védelmi rendszabályok bedolgozása érdekében azonosítani kell a biztonságért felelős személyt

(személyeket). A tervezésért, szervezésért, szakfeladatokért – így a biztonságért – felelős személyek feladatait meg kell határozni.

A tervezés, kialakítás, üzemeltetés során ismétlődő jelleggel azonosítani kell az elektronikus adatkezelő rendszert érintő fenyegetettségeket, sebezhetőségeket. A vizsgálat alapján meg kell határozni és jóvá kell hagyatni az elfogadható mértékű kockázatokat.

Az elfogadható mértékű kockázatok figyelembe vételével a kialakítás vagy változtatás fázisaihoz igazodó biztonsági követelményeket kell kialakítani és jóváhagyatni.

A biztonsági követelmény teljesülése érdekében az elektronikus adatkezelő rendszert biztonsági osztályba kell sorolni. A biztonsági osztályon belül a védelmi rendszabályok specializálása, az adatkezelő funkciókhoz történő illesztés érdekében csoportok alakíthatók ki. A biztonsági osztályokra vonatkozó általános követelményeket a honvédelmi tárca információ biztonságpolitikája határozza meg.[3] [7] Az adatok bizalmasságának, sértetlenségének vagy rendelkezésre állásának változásából, vagy az adatok mennyiségének változásából adódó halmozódási hatásból (aggregation effect) adódó kockázatokat a biztonsági osztály vagy csoport átsorolással kell ellensúlyozni.[4]

Az adatkezelő szervezeteket az alkalmazott biztonsági osztályok figyelembe vételével a jogszabályi követelménynek megfelelően szervezeti biztonsági szintekbe kell sorolni. [4] A biztonsági osztályokra és a szervezeti biztonsági szintekre vonatkozó besorolásokat időszakonként felül kell vizsgálni.

A biztonsági követelmények alapján az elektronikus adatkezelő rendszer kialakítási vagy változtatási fázisaihoz igazodóan ki kell dolgozni és jóvá kell hagyatni a védelmi rendszabályokat tartalmazó biztonsági dokumentumokat (üzemeltetés biztonsági szabályzat, elektronikus információbiztonsági szabályzat). [6] [4] Fontos adminisztratív kérdés a kétfajta szabályozás összhangjának biztosítása, mivel a NATO, EU követelmények szerinti Üzemeltetés Biztonsági Szabályzat struktúrája valószínűleg eltér a másik szabályozótól. Ugyanígy szükség van a nemzeti és a NATO, EU minősített adatok szabályozási rendjének összehangolására is, mert eltérőség esetén nehezen megoldható adminisztratív problémák jelenhetnek meg, melyet meg kell oldani az MH vonatkozó szabályozóiban, [8][9] beleértve a meglévő rendszerek szabályozásának változtatásával, a képzéssel és hatósági akkreditálással kapcsolatos feladatokat.

Minősített adatkezelő rendszerek esetében:

- NATO és EU minősített elektronikus adatkezelő rendszereknél a rendszerbiztonsági követelmények, valamint az üzemeltetési biztonsági szabályzat kialakítása az aktuális NATO, EU szabályzók, valamint a jogszabályoknak megfelelően kell, hogy történjen.
- NATO struktúrába tartozó nemzeti szervezet, vagy kirendelt erő esetén a NATO általános szabályozók mellett a NATO szervezetekre specializált követelményeknek is meg kell felelni.
- Nemzeti minősített adatkezelő rendszer esetében a biztonsági dokumentumokat a vonatkozó jogszabályok által meghatározott követelmények szerint kell kialakítani.
- NATO EU követelmények, vagy jogszabályban meghatározott esetekben a minősítési szintnek megfelelő rejtjelzést kell alkalmazni elektronikus adatkezelés esetén.[5] A

[3] A biztonsági osztályok kialakításával kapcsolatos szakmai kihívás, hogy a már idézett Ibtv. alapján elrendelt végrehajtást szabályozó rendelet hogyan fogja a törvény által meghatározott öt biztonsági osztályt definiálni [4], tekintettel arra, hogy a minősítési szintek száma négy.

[4] Az elkülönítetten kezelt adatbázisok egyesítése, illetve a kezelt adatok mennyiségének gyorsuló ütemű növekedése miatt ennek a kérdésnek általános vizsgálata, az egyes szakterületi lehetőségek feltárása és megoldások kidolgozása szükségszerűen előtérbe fog kerülni.

[5] A korábbi nemzeti követelmények alkalmazása során rejtjelzés területén az „adatkezelés” a gyakorlatban a védett terület határán túl történő elektronikus továbbításra egyszerűsödött az adatkezelés, ami az „adattárolás” érdekében végzett rejtjelzés háttérbe szorulását okozta.

rejtjelzést a hatósági követelményeknek megfelelően kell kialakítani és alkalmazása az illetékes hatóság engedélyezésével történhet.
- „Bizalmas!” és magasabb minősítési szint esetén a minősítési szintnek megfelelő, az adatkezelő eszközökre és helyszínekre vonatkozó kompromittáló kisugárzás elleni védelmi rendszabályokat kell kialakítani és fenntartani.
- Minősített adatkezelő rendszer tervezését, fejlesztését, kialakítását, üzemeltetését az akkreditáló hatóság követelményeinek figyelembevételével kell végezni.

Új elektronikus adatkezelő rendszer alkalmazásba vétele, vagy a tervezett változtatás utáni alkalmazásba vétel csak funkcionális és biztonsági ellenőrzés, az üzemeltetési és biztonsági dokumentumok ellenőrzése, és a szükséges képzések dokumentált végrehajtása után történhet.

ENGEDÉLYEZÉS

Az engedélyezési fázis lényege, hogy új vagy módosított elektronikus adatkezelő rendszerek, szolgáltatások csak engedélyezési eljárás által történő feljogosítással kerülhessenek használatba. Az engedélyezés széles körben értelmezve lehet egy hatósági eljárás keretén belül történő akkreditálás vagy műszaki ellenőrzés, helyi körben egy üzemeltetési folyamat változtatásakor a teszt eljárás áttekintése, a dokumentumok pontosításának ellenőrzése és a szükséges képzés befejezésével az új eljárás alkalmazásba vételének jóváhagyása.

Új elektronikus adatkezelő rendszer használatba vétele, vagy a változást követő használatba vétel csak a meghatározott engedélyezési eljárás sikeres lefolytatása után történhet.

A rendszerek kialakításakor a NATO, EU követelményeknek, és a jogszabályoknak megfelelően azonosítani kell az engedélyezési eljárást, az engedélyezésre feljogosított személyt.

Az elektronikus adatkezelő rendszer üzemeltetési és biztonsági dokumentumaiban egyértelműen azonosítani kell az akkreditálási, auditálási és egyéb engedélyezési jogosultságokkal rendelkező hatóságokat és szervezeteket, az alkalmazásba vétel, vagy változás engedélyezési eljárásban hatáskörrel rendelkező szerveket, szervezeteket vagy személyeket illetve a szükséges eljárásokat. A jogszabályban meghatározott információs rendszerek és a minősített elektronikus adatkezelő rendszerek használatba vétele, vagy meglévő rendszeren változások megtétele a hatósági feladatokat ellátó szervezetek, szervek követelményei szerint kialakított eljárás lefolytatása és a szükséges határozat (engedély) kiadása alapján történhet.

Az elektronikus minősített adatokat kezelő rendszert ideiglenesen más biztonsági környezetben üzemeltetni, vagy más szabályok szerint üzemeltetni csak az esetre specializált engedéllyel lehet.

Az elektronikus minősített adatokat kezelő rendszeren tesztelés csak a tesztelésre kiadott engedély birtokában hajtható végre.

Az elektronikus minősített adatokat kezelő rendszer azonos, vagy eltérő minősítésű (vagy biztonsági osztályú) adatokat kezelő rendszerrel, vagy nem minősített adatokat kezelő rendszerrel csak az összekapcsolást engedélyező eljárás után lehetséges. Az összekapcsolást biztosító rendszerre vonatkozó biztonsági szabályozás kialakítása, jóváhagyása az akkreditálási feltételek közé tartozik.

AZ ÜZEMELTETÉS BIZTONSÁGI SZEMPONTJAI ÉS FELADATAI

Az elektronikus adatkezelő rendszerek életciklusában az üzemeltetés fázis feladatai a legismertebbek, a felhasználókat is ez az időtartam szolgálja ki, de ennek ellenére rengeteg gyakorlati példa mutatja, hogy ez a legjobban „kivívásokkal teli" időszak.

Az elektronikus adatkezelő rendszerek üzemeltetése csak *jóváhagyott üzemeltetési és biztonsági dokumentumok alapján, az arra felhatalmazott személyek által történhet*. A „jóváhagyott dokumentum" kifejezésnek tartalmaznia kell azt a meghatározást is, hogy MIT kell üzemeltetni. Ez a követelmény a jóváhagyott hardver és szoftver konfigurációt, az engedélyezett hálózati összekapcsolásokat, illetve a szükséges üzemeltetési folyamatokat tartalmazza.

A felhatalmazott személyek kapcsán ki kell emelni, hogy a nemzetbiztonsági ellenőrzés és a szükséges megismerési felhatalmazások mellett kiemelt fontosságú az adott munkakör elvégzéséhez szükséges *végzettség, tudás és gyakorlati tapasztalat megléte*, mely kérdés fontosságát a napjainkban tapasztalható munkaerő elvándorlás igazol. Ugyanígy fontos a *szerződő partnerek alkalmazottainak felhatalmazása*, és a munkavégzés szabályozása, felügyelete, vagy a *távozó üzemeltető vagy biztonságért felelős személy elszámoltatása, és hozzáférési jogosultságainak azonnali visszavonása*.[6]

Az üzemeltetési és védelmi rendszabályok csak *a jóváhagyó szerv vagy szervezetek engedélyével, a szükséges dokumentálási és képzési eljárások után változtathatók*. Ez a követelmény a sok mérgelődést okozó „így szoktuk" vagy „azt mondták, így csináljam" egyszerűsítések által okozható károk megelőzését célozza.

A rendszerekért vagy szolgáltatásokért felelős vezetőknek *meg kell akadályozni a meghatározott üzemeltetési és védelmi rendszabályok egyszerűsítését, felülírását, és meg kell akadályozni az engedély nélküli változtatásokat*, így egyszerűen elkerülhető, hogy például ellenőrzés során derüljön ki, hogy a pontosnak vélt konfigurációs nyilvántartás a néhány évvel korábbi változásokat nem tartalmazza. A követelmény teljesítéséhez *kulcskérdés a szabályozott munkakör és munkavégzés, az oktatás és időszakos továbbképzés és az ellenőrzés*.

Az üzemeltető, biztonságért felelős és a felhasználói állományt a rájuk vonatkozó kötelezettségekről, feladatokról, az őket érintő *üzemeltetési és biztonsági körülmények változásáról rendszeres időnként tájékoztatni kell*. A tájékoztatással megelőzhetők az ismerethiányra visszavezethető hibák, illetve meghatározhatók a tervezett változásokkal kapcsolatos feladatok, melynek egyik legfontosabb célja a váltásos rendben dolgozó állomány naprakész ismereteinek biztosítása, illetve felhasználói oldalon a zökkenőmentes munkavégzés támogatása.

Az elektronikus adatkezelő rendszer szabályos üzemeltetése és használata, valamint *az üzemeltetési és biztonsági problémák szabályozókban rögzített módon történő jelentése minden érintett személy feladata*.

Az üzemeltetésre és biztonságra vonatkozó adatokat az elektronikus adatkezelő rendszer üzemeltetése során folyamatosan ellenőrizni, elemezni és értékelni kell. Itt nem csak az elsőre gondolt biztonsági események utáni kutatás a legfontosabb szempont.

Az üzemeltetett eszközök meghibásodásainak típusa, gyakorisága, a kiesések összetétele, a forgalmi adatok változásai, a kiszolgáló elemek terhelési mutatóinak figyelemmel kísérése, vagy csak egyszerűen a szerverterem hűtési-fűtési rendszerének vagy a földelésnek az ellenőrzése is meglepetéseket előzhet meg, illetve segítheti a megelőző jellegű karbantartások tervezését, segíti a hálózati vagy eszköz szintű amortizációs cserék vagy kiegészítések tervezését, illetve az ehhez szükséges pénzügyi és egyéb területű erőforrások tervezését.

[6] A hozzáférési jogosultságok visszavonása feladat esetenként rosszul értelmezett, mert elvonja a figyelmet arról a tényről, hogy *a munkakör elhagyásának, és nem a munkahely elhagyásának esetét kell kezelni*.

Az elektronikus adatkezelő rendszert és üzemeltetési környezetét *meghatározott időszakonként, valamint változások előkészítésekor kockázatelemzéssel kell vizsgálni*.

Az elektronikus adatkezelő rendszereket specifikusan, az adott rendszerre vonatkozó rendben *biztonsági ellenőrzéseknek kell alávetni*. A biztonsági ellenőrzéseknek szükségszerűen át kell fogni az információbiztonság összes területét.

A kezelt adatok, a biztonsági környezet, a csatlakozó rendszerek függvényében ez *az ellenőrzés inkább ellenőrzési rendet kell, hogy jelentsen*. Az üzemeltető állomány ellenőrzésén kívül ide kell sorolni a különböző szintű elöljárói ellenőrzéseket és célellenőrzéseket, a hatósági ellenőrzéseket, illetékesség esetén a NATO, EU különböző biztonsági szervezeteinek ellenőrzéseit, ami az adminisztratív ellenőrzés mellett a mérnöki szintű elemzést, auditot, vagy összekapcsolt rendszerek esetén külső sebezhetőség elemzést is tartalmazhat, mely ellenőrzési típusok még tovább specializálhatók.

Változások csak jóváhagyott terv, kockázatelemzés és teszt, valamint tájékoztatás és képzés után végezhetők.

A RENDSZERBŐL TÖRTÉNŐ KIVONÁS BIZTONSÁGI SZEMPONTJAI ÉS FELADATAI

Kevés esetben mondható ki, hogy meghatározott időszakra létrehozott elektronikus adatkezelő rendszer – annak elemeivel együtt – az adott feladat teljesítése után valóban eléri a rendszerből történő kivonást, így biztonsági szempontból kiemelt fontosságú az adatkezelő rendszerekkel és az adatokkal való teendők említése.

Az elektronikus adatkezelő rendszer üzemeltetésből történő kivonása csak *az engedélyező szerv, szervezetek vagy személyek engedélyével történhet*. Az engedély nélküli végzett műveletek eredménye könnyen okozhat hálózati szinten váratlan eseményeket, problémákat főleg a szükséges üzemeltetési információk hiánya, rendszerdokumentumok pontatlansága esetén. Emiatt nyilvánvaló, hogy egy hardver vagy szoftver kivonása a rendszerből, vagy egy rendszer leállítása *csak az egész információs környezet ismeretében a szükséges előkészítési, és összehangolási lépések után végezhető*.

A rendszerből történő kivonást *jóváhagyott eljárással kell végrehajtani*, melynek tartalmaznia kell az *összes dokumentummal és adattal, valamint az elektronikus adatkezelő rendszer hardver és szoftver elemeivel kapcsolatos biztonsági követelményeket* és védelmi rendszabályokat.

A rendszerből történő kivonás tervezésekor *meg kell határozni a kezelt adatok biztonsági osztályának megfelelő eljárást az adatok más rendszerbe történő áttelepítéséhez, tárolásához vagy archiválásához*.

A rendszerből történő kivonás szakfeladatait *csak az arra feljogosított személyek végezhetik*. Az eszközökkel kapcsolatos műszaki feladatok, adatmentések során előfordulhat nagymennyiségű üzemeltetési vagy felhasználói adattal történő művelet, ami lényegesen nagyobb információs katasztrófát okozhat, mint korábban egy felhasználó által elérhető adatokkal történő biztonsági probléma.

A rendszerből történő kivonáskor meg kell határozni a hardver és szoftver elemekre vonatkozó újrahasznosítási, adattörlési, megsemmisítési vagy egyes műveleteket tiltó rendszabályokat. Az elektronikus adatok megbízható törlése külön tárgyalást igénylő témakör. Az információs kockázatok egy bizonyos szintjén már előfordulhat, hogy *a szervezeti érdek csak a fizikai megsemmisítést tartja elfogadhatónak, ami külön technikai megoldásokat fog igényelni*, mely megoldások erőforrás szükséglete nem biztos, hogy minden esetben bekerült a „tervezői látókörbe”.

Tárolás vagy archiválás esetén *meg kell tervezni és ki kell alakítani a szükséges biztonsági környezetet, és adatkezelő infrastruktúrát úgy, hogy bekövetkező technikai és eljárási*

változások esetén is biztosított legyen az adatok hozzáférése és kezelhetősége. A technológia rohamos idejű fejlődése néhány év alatt is képes váratlan helyzeteket produkálni, amelynek egyik jelensége lehet, hogy adott fájlformátum, megjelenítési mód, vagy szoftver a korszerűbb információs környezetben már nem alkalmazható, csatlakozási felületek, átalakítók már kezelhetők. Ilyen esetben meglepetéseket okozhat például az elektronikus hitelesítés szolgáltatás esetében a szolgáltatót terhelő, jogszabály által meghatározott tízéves visszakereshetőségi kötelezettség, vagy rejtjelzett adatok tárolása esetén a kulcsmenedzsment kérdések bonyolultsága. Emiatt külön feladat – és nem csak biztonsági szempontból tekinthető kihívásnak – az adatok és az adatkezelési környezet huzamosabb időn keresztül történő biztosítása.

ÖSSZEGZÉS, KÖVETKEZTETÉSEK

A cikk a Szabályzatban megfogalmazandó fontosabb elektronikus információ biztonsági kérdések megvilágítását célozta a híradó és informatikai szakterületi feladatok támogatása érdekében.

Az életciklushoz kötve bemutatott fontosabb biztonsági követelmények és szempontok jól mutatják a védelmi rendszabályok sokszínűségét, bonyolultságát. Nyilvánvaló, hogy *a biztonsági kockázatok kizárásához ilyen szintű elektronikus információvédelmi rendszabályok nem lehetnek elégségesek*, illetve az adatkezelés sajátosságai sem teszik lehetővé, hogy a harcászati rádiók szintjétől a szövetségesi együttműködést biztosító stratégiai szintű szolgáltatásokat együttesen ilyen röviden lehessen bemutatni.

Összefoglalásként elmondható, hogy az elektronikus adatkezelő rendszerek kialakítása üzemeltetése és rendszerből történő kivonása *lényegesen bonyolultabb feladat, mint az a köztudatban ismert*. Az összetett üzemeltetés támogató feladatok előrelátó erőforrás tervezés hiányában csak ideig-óráig lehetnek sikeresek, illetve az is látható, hogy *mekkora jelentősége van a pontosan megfogalmazott követelményeknek*, ami a híradó és informatikai szakfeladatok hadműveleti területről történő támogatásának fontosságát húzza alá.

A kockázatelemezés és kezelés, az ellenőrzés, a szabályozás, a felelősségek azonosítása, a változások követése és rögzítése, valamint a képzés *az életciklus állomásokon egységesen megjelenő feladat kell, hogy legyen*. A napi életben előállhat olyan helyzet, amikor *a felső szintű szabályozó keretjellege miatt pontosan nem alkalmazható a katonai képességek híradó és informatikai rendszereinek védelmére*. Ilyen esetekben fontos szerepe van a szakképzett biztonsági menedzsmentnek, annak érdekében, hogy *kidolgozzák a szükséges helyettesítő megoldásokat, azokat ellenőrizzék, és a megoldás engedélyezése érdekében végezzék az illetékes hatóságok felé a szükséges adminisztratív feladatokat*. Ez a megoldás lényegesen hatékonyabb, mint az adott probléma megküldése a hatóság felé, mert *az esetek nagy részében a katonai specialitások, működési jellemzők vagy a környezet pontos ismerete nélkül a legnagyobb jóindulattal sem könnyű jó szakmai tanácsokat adni*.

A feladatok összetettsége felvet egy újabb szempontot: *a szervezeten belüli és a szervezetek közötti együttműködés kérdését* és fontosságát. Korábban a kevesebb feldolgozott adat, kevesebb hálózati szolgáltatás miatt viszonylag egyszerűbb volt a honvédelmi szerv vezetőjének helyzete. Az üzemeltető informatikai állomány, a híradó eszközök és komplexumok kezelő állomány, valamint a számítástechnikai titokvédelmi felelős kijelölésével a feladatok nagy része „kipipálható” volt. Napjainkban ez a helyzet lényegesen bonyolultabbá vált. Gyakori az a helyzet, hogy a híradó és informatikai üzemeltetők, a biztonságért felelős személyek más szervnél vagy szervezetnél találhatók, illetve *a hálózatok szolgáltatásai és üzemeltetés szervezeti határokon átnyúló feladatokat jelent*. Ezen összetettség miatt a szervezeti vezetők feladata is megváltozott: az eddig elégséges sorszámos rendelkezés kiadása helyett a szervezeti együttműködés kérdéseit is kezelni kell, ráadásul nem csak vezetői szinten történő

kapcsolattartásra szűkítve, mert a hálózatokba történő gondolkodás megköveteli az üzemeltető és biztonsági állomány közvetlen kapcsolattartását is!

A szakfeladatok bemutatása rámutat arra is, hogy szükség van a terminológiai kérdések fontosságának említésére. A hadtudomány egyik soros feladata a szakkifejezések megnyugtató rendezése, beleértve a híradó és informatikai szakterületet is.

Jelen cikk megjelenésekor a szakkifejezések kérdése még nyitott, így szükség van annak jelzésére, hogy az alkalmazott „elektronikus adatkezelő rendszer" kifejezés a tervezett Szabályzatban alkalmazott, egyeztetett terminológiai gyakorlatnak megfelelő kifejezéssel helyettesítendő, tartalmi szempontból lefedve az elektronikus adatkezelés területeit.

Felhasznált irodalom

[1] A Magyar Honvédség Informatikai Szabályzata, Ált/210, 1993

[2] 218/2013 HVKF paranccsal módosított 209/2013 HVKF parancs a Magyar Honvédség Híradó - Informatikai Szabályzatának kidolgozásáról

[3] 346/2010. (XII. 28.) Korm. rendelet a kormányzati célú hálózatokról, 6. §, 28-31. §.

[4] 2013. évi L. törvény az állami és önkormányzati szervek elektronikus információbiztonságáról (Ibtv.)

[5] 90/2010. (III. 26.) Korm. rendelet a Nemzeti Biztonsági Felügyelet működésének, valamint a minősített adat kezelésének rendjéről

[6] 161/2010. (V. 6.) Korm. rendelet a minősített adat elektronikus biztonságának, valamint a rejtjeltevékenység engedélyezésének és hatósági felügyeletének részletes szabályairól

[7] 94/2009. (XI. 27.) HM utasítás a honvédelmi tárca információbiztonság politikájáról, 15. §.

[8] A Honvéd Vezérkar híradó, informatikai és információvédelmi csoportfőnökének 9/2012. (HK 14.) HVK HIICSF szakutasítása a Minősített Elektronikus Adatkezelő Rendszer Üzemeltetés Biztonsági Szabályzatára vonatkozó általános követelményekről

[9] A Honvéd Vezérkar híradó, informatikai és információvédelmi csoportfőnökének 10/2012. (HK 14.) HVK HIICSF szakutasítása a Minősített Elektronikus Adatkezelő Rendszer ellenőrzésére vonatkozó általános követelményekről, 5, 7, és 10. p.